Claims

[1] A rijndael block cipher apparatus comprising:
a round operation unit for transforming a 128-bit input key into a 128-bit round key for encryption or decryption, and storing the 128-bit round key according to a value of a mode signal from a time when a round operation start signal, a round number signal and a bit selection signal for dividing the 128-bit input data into upper 64 bits and lower 64 bits and selecting the upper or lower 64 bits are inputted after an encryption or decryption operation start signal and the mode signal are inputted, encrypting the 128-bit input data by dividing the 128-bit input data into the upper 64 bits and the lower 64 bits and by performing a round operation which is composed of transforms of shift_row, substitution, mixcolumn and add-round-key with respect to the divided upper 64 bits and lower b4 bits, respectively, and decrypting the 128-bit input data by dividing the 128-bit input data into the upper 64 bits and the lower 64 bits and by performing a round operation which is composed of transforms of inverse-shift_row, inverse substitution, add-round-key and inverse mixcolumn with respect to the divided upper 64 bits and lower b4 bits, respectively;
a round operation control unit for controlling the round operation of the round operation unit by transmitting the round operation start signal, the round number signal and the bit selection signal for dividing the 128-bit input data into the upper 64 bits and lower 64 bits and selecting the upper or lower 64 bits to the round operation unit from a time when the encryption or decryption operation start signal and the mode signal are inputted;
a 64-bit data register for storing intermediate encryption or decryption data of the upper 64-bit input data generated during each round operation performed by the round operation unit; and
a 128-bit data register for storing intermediate encryption or decryption data of the lower 64-bit input data generated during each round operation performed by the round operation unit as its lower 64 bits, and storing the encryption or decryption data generated as a result of a last round operation and stored in the 64-bit data register as its upper 64-bit data.

[2] The apparatus as claimed in claim 1, wherein the round operation unit comprises:
a round key generation unit for transforming the 128-bit input key into the 128-bit round key RK for encryption or decryption according to the value of the

mode signal inputted through a bus and storing the 128-bit round key in an internal 128-bit round key register if the round operation start signal and the round number signal are inputted from the round operation control unit;
a shift/inverse-shift_row transform unit for performing a byte-shift of the upper 64 bits and the lower 64 bits divided from the 128-bit input data inputted through the bus by different numbers according to the value of the mode signal inputted through the bus if the round operation start signal and the bit selection signal are inputted from the round operation control unit, and outputting the byte-shifted upper 64 bits and lower 64 bits through a first multiplexer the output of which is controlled according to the value of the bit selection signal;
a substitution/inverse-substitution transform unit for performing a substitution or an inverse substitution of the upper 64-bit data and the lower 64-bit data outputted from the shift/inverse-shift_row transform unit using a substitution box (S-box) or an inverse-substitution box (SI-box) that provides a one-byte output with respect to a one-byte input;
a first demultiplexer for outputting the upper 64-bit data or the lower 64-bit data outputted from the substitution/inverse-substitution transform unit through either of its encryption output terminal and its decryption output terminal according to the value of the mode signal;
a mix/inverse-mixcolumn transform unit for performing a mixcolumn of the upper 64-bit data or the lower 64-bit data inputted through the encryption output terminal of the first demultiplexer, or performing an inverse mixcolumn of the upper 64-bit data or the lower 64-bit data that has been add-round-key-transformed;
a second demultiplexer for outputting the upper 64-bit data or the lower 64-bit data outputted from the mix/inverse-mixcolumn transform unit through either of its encryption output terminal and its decryption output terminal according to the value of the mode signal;
an add-round-key transform unit for performing an addition of the upper 64-bit data or the lower 64-bit data inputted through the decryption output terminal of the first demultiplexer or through the encryption output terminal of the second demultiplexer to the 128-bit round key RK for encryption or decryption outputted from the round key generation unit; and
a third demultiplexer for outputting the upper 64-bit data or the lower 64-bit data outputted from the add-round-key transform unit through either of its encryption

output terminal and its decryption output terminal according to the value of the mode signal.

[3] The apparatus as claimed in claim 1 or 2, wherein if the four-clock or three-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data outputted from the substitution/ inverse-substitution transform unit to the first demultiplexer is stored in the 64-bit data register, and the lower 64-bit data outputted is stored as lower 64-bit data of the 128-bit data register.

[4] The apparatus as claimed in claim 1 or 2, wherein if the four-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data outputted from the mix/ inverse-mixcolumn transform unit to the second demultiplexer is stored in the 64-bit data register, and the lower 64-bit data outputted is stored as lower 64-bit data of the 128-bit data register.

[5] The apparatus as claimed in claim 1 or 2, wherein if the four-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data for encryption outputted from the add-round-key transform unit to the third demultiplexer is stored as upper 64-bit data of the 128-bit data register, and the lower 64-bit data for encryption is stored as lower 64-bit data of the 128-bit data register.

[6] The apparatus as claimed in claim 1 or 2, wherein if the four-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data for decryption outputted from the add-round-key transform unit to the third demultiplexer is stored in the 64-bit data register, and the lower 64-bit data for decryption is stored as lower 64-bit data of the 128-bit data register.

[7] The apparatus as claimed in claim 1 or 2, wherein if the four-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the inverse-mixcolumn-transformed upper 64-bit data outputted from the mix/inverse-mixcolumn transform unit to the second demultiplexer is stored as upper 64-bit data of the 128-bit data register, and the inverse-mixcolumn-transformed lower 64-bit data is stored as lower 64-bit data of the 128-bit data register.

[8] The apparatus as claimed in claim 1 or 2, wherein if the three-clock round operation start signal is inputted from the round operation control unit to the

round operation unit, the upper 64-bit data for encryption inverse-mixcolumn-transformed and then outputted from the add-round-key transform unit to the third demultiplexer is stored in the 64-bit data register, and then if a last third clock becomes '1', the upper 64-bit data for encryption is stored as upper 64-bit data of the 128-bit data register, and the lower 64-bit data for encryption is stored as lower 64-bit data of the 128-bit data register.

[9] The apparatus as claimed in claim 1 or 2, wherein if the three-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data add-round-key-transformed, inverse-mixcolumn-transformed, and then outputted from the mix/inverse-mixcolumn transform unit to the second demultiplexer is stored in the 64-bit data register, and then if a last third clock becomes '1', the inverse-mixcolumn-transformed upper 64-bit data is stored as upper 64-bit data of the 128-bit data register, and the inverse-mixcolumn-transformed lower 64-bit data is stored as lower 64-bit data of the 128-bit data register.

[10] The apparatus as claimed in claim 1 or 2, wherein if the two-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data for encryption shift_row-trasnformed, substitution-transformed, mixcolumn-transformed, and then outputted from the add-round-key transform unit to the third demultiplexer is stored in the 64-bit data register, and then if a last second clock becomes '1', the upper 64-bit data for encryption is stored as upper 64-bit data of the 128-bit data register, and the lower 64-bit data for encryption is stored as lower 64-bit data of the 128-bit data register.

[11] The apparatus as claimed in claim 1 or 2, wherein if the two-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the upper 64-bit data inverse-shift_row-trasnformed, inverse-substitution-transformed, add-round-key-transformed, and then inverse-mixcolumn-transformed and outputted from the mix/inverse-mixcolumn transform unit to the second demultiplexer is stored in the 64-bit data register, and then if a last second clock becomes '1', the inverse-mixcolumn-transformed upper 64-bit data is stored as upper 64-bit data of the 128-bit data register, and the inverse-mixcolumn-transformed lower 64-bit data is stored as lower 64-bit data of the 128-bit data register.

[12] The apparatus as claimed in claim 2, wherein the round key generation unit

comprises:

a 128-bit prekey register for storing the 128-bit input key inputted through the bus as a prekey for transforming the 128-bit input key into the 128-bit round key RK for encryption or decryption, and storing the 128-bit round key RK generated after each round operation as a prekey for generating a round key RK used in a next round operation;

a 128-bit key register for storing the 128-bit round key RK for encryption or decryption for each round operation;

a constant storage unit for storing constant values Rcon determined according to the order of the round indicated by the round number signal inputted from the round operation control unit;

a second multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selecting and outputting one of 32-bit keys for encryption or decryption inputted from the 128-bit prekey register and the 128-bit round key register;

a shifter for performing a cyclic shift of the 32-bit key inputted through the second multiplexer to the left by one byte;

a substitution transform unit, composed of substitution boxes (S-boxes) for performing a substitution operation, for performing the substitution of the 32-bit key shifted by the shifter;

a first XOR gate for performing an XOR operation of the most significant byte of the 32-bit key outputted from the substitution transform unit with the constant value stored in the constant storage unit; and

a round XOR operation unit for newly generating the 128-bit round key RK for encryption or decryption to be stored in the 128-bit round key register for each round of the round operation by performing an XOR operation using a 32-bit value obtained by adding output bits of the first XOR gate to the remaining 24 bits except for the most significant byte of the substitution transform unit, the 128-bit prekey of the previous round stored in the 128-bit prekey register 111, and the 128-bit round key RK of the new round stored in the 128-bit round key register.

[13] The apparatus as claimed in claim 12, wherein if the four-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the round XOR operation unit of the round key generation unit generates the encryption round key in a period of four clocks; and

wherein the round XOR operation unit comprises:

a second XOR gate for generating the most significant 32-bit round key RKO of the 128-bit round key for encryption or decryption of the new round by performing an XOR operation of the 32-bit value obtained by adding the output bits of the first XOR gate to the remaining 24 bits except for the most significant byte of the substitution transform unit, with the most significant 32-bit value PKO of the 128-bit round key of the previous round, if the first clock of the encryption round operation start signal becomes '1';

a third XOR gate for generating a 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for encryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RKO of the 128-bit round key of the new round with a 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits of the 128-bit round key of the previous round, and generating the 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for decryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key PKO of the 128-bit round key of the previous round with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits, if the second clock of the encryption round operation start signal becomes '1';

a third multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the third XOR gate;

a fourth XOR gate for generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for encryption of the new round by performing an XOR operation of the 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key of the new round with a 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the 128-bit round key of the previous round, and generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 95th bit to 64th bit) round key PK1 of the 128-bit round key of the previous round with the next 32-bit (i.e., 63rd bit to 32nd bit) round key PK2, if the third clock of the encryption round operation start signal becomes '1';

a fourth multiplexer for being is controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fourth XOR gate;

a fifth XOR gate for generating a 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for encryption of the new round by performing an XOR operation of the 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key of the new round with a 32-bit (i.e., 31st bit to 0th bit) round key PK3 of the 128-bit round key of the previous round, and generating a 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the 128-bit round key of the previous round with the next 32-bit (i.e., 31st bit to 0th bit) round key PK3, if the fourth clock of the encryption round operation start signal becomes '1'; and

a fifth multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fifth XOR gate.

[14] The apparatus as claimed in claim 12, wherein if the three-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the round XOR operation unit of the round key generation unit generates the encryption round key in a period of two clocks; and

wherein the round XOR operation unit comprises:

a second XOR gate for generating the most significant 32-bit round key RKO of the 128-bit round key for encryption or decryption of the new round by performing an XOR operation of the 32-bit value obtained by adding the output bits of the first XOR gate to the remaining 24 bits except for the most significant byte of the substitution transform unit, with the most significant 32-bit value PKO of the 128-bit round key of the previous round, if the first clock of the encryption round operation start signal becomes '1' ;

a third XOR gate for generating a 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for encryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RKO of the 128-bit round key of the new round with a 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits of the 128-bit round key of the previous round, and generating the 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for decryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key PKO of the 128-bit round key of the previous round with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits, if the second clock of the encryption round operation start signal becomes '1' ;

a third multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the third XOR gate;

a fourth XOR gate for generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for encryption of the new round by performing an XOR operation of a resultant value

(RK0 ⊕ PK1),

which is obtained by the third XOR gate's XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RK0 of the 128-bit round key of the new round with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32 bits of the 128-bit round key of the previous round, with the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the previous round, and generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 95th bit to 64th bit) round key PK1 of the 128-bit round key of the previous round with the next 32-bit (i.e., 63rd bit to 32nd bit) round key PK2, if the second clock of the encryption round operation start signal becomes '1' ;

a fourth multiplexer for being is controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fourth XOR gate;

a fifth XOR gate for generating a 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for encryption of the new round by performing an XOR operation of the resultant value

(RK0 ⊕ PK1),

which is obtained by the fourth XOR gate's XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RK0 of the 128-bit round key of the new round that has been XORed by the third XOR gate with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32 bits of the 128-bit round key of the previous round, with the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the previous round to produce a resultant value

(RK0 ⊕ PK1 ⊕ PK2)

of XOR operation, and then by performing an XOR operation of the resultant value

(RKO ⊕ PK1 ⊕ PK2)
with the 32-bit (31 st bit to 0th bit) round key PK3 of the previous round, and generating the 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the 128-bit round key of the previous round with the next 32-bit (i.e., 31st bit to 0th bit) round key PK3, if the second clock of the encryption round operation start signal becomes '1' ; and
a fifth multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fifth XOR gate.

[15] The apparatus as claimed in claim 12, wherein if the two-clock round operation start signal is inputted from the round operation control unit to the round operation unit, the round XOR operation unit of the round key generation unit generates the encryption round key in a period of one clock; and
wherein the round XOR operation unit comprises:
a second XOR gate for generating the most significant 32-bit round key RKO of the 128-bit round key for encryption or decryption of the new round by performing an XOR operation of the 32-bit value obtained by adding the output bits of the first XOR gate to the remaining 24 bits except for the most significant byte of the substitution transform unit, with the most significant 32-bit value PKO of the 128-bit round key of the previous round, in a state that the encryption round operation start signal is inputted and simultaneously, the clock becomes '0' ;
a third XOR gate for generating a 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for encryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RKO of the 128-bit round key of the new round with a 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits of the 128-bit round key of the previous round, and generating the 32-bit (i.e., 95th bit to 64th bit) round key RK1 of the 128-bit round key for decryption of the new round by performing an XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key PKO of the 128-bit round key of the previous round with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32bits, if the first clock of the encryption round operation start signal becomes '1' ;
a third multiplexer for being controlled according to the value of the mode signal

inputted through the bus, and selectively determining input signals of the third XOR gate;

a fourth XOR gate for generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for encryption of the new round by performing an XOR operation of a resultant value

(RK0 ⊕ PK1),

which is obtained by the third XOR gate's XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RK0 of the 128-bit round key of the new round with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32 bits of the 128-bit round key of the previous round, with the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the previous round, and generating a 32-bit (i.e., 63rd bit to 32nd bit) round key RK2 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 95th bit to 64th bit) round key PK1 of the 128-bit round key of the previous round with the next 32-bit (i.e., 63rd bit to 32nd bit) round key PK2, if the first clock of the encryption round operation start signal becomes '1' ;

a fourth multiplexer for being is controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fourth XOR gate;

a fifth XOR gate for generating a 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for encryption of the new round by performing an XOR operation of the resultant value

(RK0 ⊕ PK1),

which is obtained by the fourth XOR gate's XOR operation of the most significant 32-bit (i.e., 127th bit to 96th bit) round key RK0 of the 128-bit round key of the new round that has been XORed by the third XOR gate with the 32-bit (i.e., 95th bit to 64th bit) round key PK1 next to the most significant 32 bits of the 128-bit round key of the previous round, with the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the previous round to produce a resultant value

(RK0 ⊕ PK1 ⊕ PK2)

of XOR operation, and then by performing an XOR operation of the resultant value

(RK0 ⊕ PK1 ⊕ PK2)

with the 32-bit (31 st bit to 0th bit) round key PK3 of the previous round, and generating the 32-bit (i.e., 31st bit to 0th bit) round key RK3 of the 128-bit round key for decryption of the new round by performing an XOR operation of the 32-bit (i.e., 63rd bit to 32nd bit) round key PK2 of the 128-bit round key of the previous round with the next 32-bit (i.e., 31st bit to 0th bit) round key PK3, if the first clock of the encryption round operation start signal becomes '1' ; and a fifth multiplexer for being controlled according to the value of the mode signal inputted through the bus, and selectively determining input signals of the fifth XOR gate.

[16] A rijndael block encryption method comprising the steps of:
if a four-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for encryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1', and storing the 128-bit round key in an internal 128-bit round key register;
if the four-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-shift of upper 64-bit data of 128-bit input data inputted through the bus and outputting the byte-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1', and a substitution/ inverse-substitution transform unit successively performing a substitution of the upper 64-bit data, outputting the substituted upper 64-bit data to a first demultiplexer, and storing the substituted upper 64-bit data in a 64-bit data register;
when a second clock of the round operation start signal becomes '1', a mix/ inverse-mixcolumn transform unit performing a mixcolumn of the upper 64-bit data outputted through an encryption output terminal of the first demultiplexer and stored in the 64-bit data register, outputting the mixcolumn-transformed upper 64-bit data to a second demultiplexer, and storing the mixcolumn-transformed upper 64-bit data in the 64-bit data register, the shift/ inverse-shift_row transform unit simultaneously performing a byte-shift of lower 64-bit data of the 128-bit input data inputted through the bus and outputting the byte-shifted lower 64-bit data through the first multiplexer, and the substitution/ inverse-substitution transform unit successively performing a substitution of the

lower 64-bit data, outputting the substituted lower 64-bit data to the first demultiplexer, and storing the substituted lower 64-bit data in lower 64 bits of a 128-bit data register;

when a third clock of the round operation start signal becomes '1', an add-round-key transform unit performing an addition of the upper 64-bit data outputted through an encryption output terminal of the second demultiplexer and stored in the 64-bit data register to upper 64-bit round key generated by the round key generation unit and storing the added upper 64-bit data in upper 64 bits of the 128-bit data register, and a mix/inverse-mixcolumn transform unit simultaneously performing a mixcolumn of the lower 64-bit data outputted through the encryption output terminal of the first demultiplexer and stored in the 128-bit data register, outputting the mixcolumn-transformed lower 64-bit data to the second demultiplexer, and storing the mixcolumn-transformed lower 64-bit data in the lower 64 bits of the 128-bit data register; and

when a fourth clock of the round operation start signal becomes '1', the add-round-key transform unit performing an addition of the lower 64-bit data outputted through the encryption output terminal of the second demultiplexer and stored in the 128-bit data register to lower 64-bit round key generated by the round key generation unit and storing the added lower 64-bit data in the lower 64 bits of the 128-bit data register.

[17] The encryption method as claimed in claim 16, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for encryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for encryption is generated in a period of four clocks of the round operation start signal.

[18] A rijndael block decryption method comprising the steps of:

if a four-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for decryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1' , and storing the 128-bit round key in an internal 128-bit round key register;

if the four-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-inverse-shift of upper 64-bit data of 128-bit input data inputted through the bus and outputting the byte-inverse-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1', and a substitution/inverse-substitution transform unit successively performing an inverse substitution of the upper 64-bit data, outputting the inverse-substituted upper 64-bit data to a first demultiplexer, and storing the inverse-substituted upper 64-bit data in a 64-bit data register;
when a second clock of the round operation start signal becomes '1', an add-round-key transform unit performing an addition of the upper 64-bit data outputted through a decryption output terminal of the first demultiplexer and stored in the 64-bit data register to upper 64-bit round key generated by the round key generation unit, outputting the added upper 64-bit data to a third demultiplexer, and storing the added upper 64-bit data in the 64-bit data register, the shift/inverse-shift_row transform unit simultaneously performing a byte-inverse-shift of lower 64-bit data of the 128-bit input data inputted through the bus, and outputting the byte-inverse-shifted lower 64-bit data through the first multiplexer, and the substitution/inverse-substitution transform unit successively performing an inverse substitution of the lower 64-bit data, outputting the inverse-substituted lower 64-bit data to the first demultiplexer, and storing the inverse-substituted lower 64-bit data in lower 64 bits of a 128-bit data register;
when a third clock of the round operation start signal becomes '1', a mix/inverse-mixcolumn transform unit performing an inverse mixcolumn of the upper 64-bit data outputted through a decryption output terminal of the third demultiplexer and stored in the 64-bit data register, outputting the inverse-mixcolumn-transformed upper 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed upper 64-bit data in upper 64 bits of the 128-bit data register, and the add-round-key transform unit simultaneously performing an addition of the lower 64-bit data outputted through the decryption output terminal of the first demultiplexer and stored in the 128-bit data register to lower 64-bit round key generated by the round key generation unit, outputting the added lower 64-bit data through the third demultiplexer, and storing the added lower 64-bit data in the lower 64 bits of the 128-bit data register; and
when a fourth clock of the round operation start signal becomes '1', the mix/

inverse-mixcolumn transform unit performing an inverse mixcolumn of the lower 64-bit data outputted through the decryption output terminal of the third demultiplexer and stored in the 128-bit data register, outputting the inverse-mixcolumn-transformed lower 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed lower 64-bit data in the lower 64 bits of the 128-bit data register.

[19] The decryption method as claimed in claim 18, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for decryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for decryption is generated in a period of two clocks of the round operation start signal.

[20] A rijndael block encryption method comprising the steps of:
if a three-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for encryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1', and storing the 128-bit round key in an internal 128-bit round key register;
if the three-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-shift of upper 64-bit data of 128-bit input data inputted through the bus and outputting the byte-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1', and a substitution/inverse-substitution transform unit successively performing a substitution of the upper 64-bit data, outputting the substituted upper 64-bit data to a first demultiplexer, and storing the substituted upper 64-bit data in a 64-bit data register;
when a second clock of the round operation start signal becomes '1', a mix/inverse-mixcolumn transform unit performing a mixcolumn of the upper 64-bit data outputted through an encryption output terminal of the first demultiplexer and stored in the 64-bit data register, and outputting the mixcolumn-transformed upper 64-bit data to a second demultiplexer, an add-round-key transform unit successively performing an addition of this upper 64-bit data to an upper 64-bit

round key generated by the round key generation unit, and storing the added upper 64-bit data in the 64-bit data register, the shift/inverse-shift_row transform unit simultaneously performing a byte-shift of lower 64-bit data of the 128-bit input data inputted through the bus, and outputting the byte-shifted lower 64-bit data through the first multiplexer, and the substitution/inverse-substitution transform unit successively performing a substitution of the lower 64-bit data, outputting the substituted lower 64-bit data to the first demultiplexer, and storing the substituted lower 64-bit data in lower 64 bits of a 128-bit data register; and when a third clock of the round operation start signal becomes '1', storing the 64-bit data added and then stored in the 64-bit data register in upper 64 bits of the 128-bit data register, the mix/inverse-mixcolumn transform unit simultaneously performing a mixcolumn of the lower 64-bit data outputted through the encryption output terminal of the first demultiplexer and stored in the 128-bit data register, and outputting the mixcolumn-transformed lower 64-bit data to the second demultiplexer, and the add-round-key transform unit successively performing an addition of the lower 64-bit data to lower 64-bit round key generated by the round key generation unit, and storing the added lower 64-bit data in the lower 64 bits of the 128-bit data register.

[21] The encryption method as claimed in claim 20, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for encryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for encryption is generated in a period of two clocks of the round operation start signal.

[22] A rijndael block decryption method comprising the steps of:

if a three-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for decryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1', and storing the 128-bit round key in an internal 128-bit round key register;

if the three-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-inverse-shift of upper 64-bit data of 128-bit input data inputted through the bus, and outputting the byte-inverse-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1', and a substitution/inverse-substitution transform unit successively performing an inverse substitution of the upper 64-bit data, outputting the inverse-substituted upper 64-bit data to a first demultiplexer, and storing the inverse-substituted upper 64-bit data in a 64-bit data register;

when a second clock of the round operation start signal becomes '1', an add-round-key transform unit performing an addition of the upper 64-bit data outputted through a decryption output terminal of the first demultiplexer and stored in the 64-bit data register to upper 64-bit round key generated by the round key generation unit, and outputting the added upper 64-bit data to a third demultiplexer, a mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added upper 64-bit data, outputting the inverse-mixcolumn-transformed upper 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed upper 64-bit data in the 64-bit data register, the shift/inverse-shift_row transform unit simultaneously performing a byte-inverse-shift of lower 64-bit data of the 128-bit input data inputted through the bus, and outputting the byte-inverse-shifted lower 64-bit data through the first multiplexer, and the substitution/inverse-substitution transform unit successively performing an inverse substitution of the lower 64-bit data, outputting the inverse-substituted lower 64-bit data to the first demultiplexer, and storing the inverse-substituted lower 64-bit data in lower 64 bits of a 128-bit data register; and

when a third clock of the round operation start signal becomes '1', the add-round-key transform unit performing an addition of the lower 64-bit data outp utted through the decryption output terminal of the first demultiplexer and stored in the 128-bit data register to lower 64-bit round key generated by the round key generation unit and outputting the added lower 64-bit data to the third demultiplexer, the mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added lower 64-bit data, outputting the inverse-mixcolumn-transformed lower 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed lower 64-bit data in the lower 64 bits of the 128-bit data register, and simultaneously storing the upper 64-bit data stored in the 64-bit data register in upper 64 bits of the 128-bit data register.

[23] The decryption method as claimed in claim 22, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for decryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for decryption is generated in a period of two clocks of the round operation start signal.

[24] A rijndael block encryption method comprising the steps of:
if a two-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for encryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1' , and storing the 128-bit round key in an internal 128-bit round key register;
if the two-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-shift of upper 64-bit data of 128-bit input data inputted through the bus and outputting the byte-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1' , a substitution/ inverse-substitution transform unit successively performing a substitution of the upper 64-bit data, and outputting the substituted upper 64-bit data through a first demultiplexer, a mix/inverse-mixcolumn transform unit performing a mixcolumn of the upper 64-bit data outputted through an encryption output terminal of the first demultiplexer, and outputting the mixcolumn-transformed upper 64-bit data to a second demultiplexer, and an add-round-key transform unit successively performing an addition of this upper 64-bit data to an upper 64-bit round key generated by the round key generation unit, and storing the added upper 64-bit data in a 64-bit data register; and
when a second clock of the round operation start signal becomes '1' , the shift/ inverse-shift_row transform unit performing a byte-shift of lower 64-bit data of the 128-bit input data inputted through the bus and outputting the byte-shifted lower 64-bit data through the first multiplexer, and the substitution/ inverse-substitution transform unit successively performing a substitution of the lower 64-bit data, and outputting the substituted lower 64-bit data to the first de-

multiplexer, the mix/inverse-mixcolumn transform unit successively performing a mixcolumn of the lower 64-bit data, and outputting the mixcolumn-transformed lower 64-bit data to the second demultiplexer, the add-round-key transform unit successively performing an addition of this lower 64-bit data to lower 64-bit round key generated by the round key generation unit, and storing the added lower 64-bit data in lower 64 bits of a 128-bit data register, and simultaneously storing the upper 64-bit data stored in the 64-bit data register in upper 64 bits of the 128-bit data register.

[25] The encryption method as claimed in claim 24, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for encryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for encryption is generated in a period of one clock of the round operation start signal.

[26] A rijndael block decryption method comprising the steps of:

if a two-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for decryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes '1', and storing the 128-bit round key in an internal 128-bit round key register;

if the two-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-inverse-shift of upper 64-bit data of 128-bit input data inputted through the bus, and outputting the byte-inverse-shifted upper 64-bit data through a first multiplexer when the first clock becomes '1', a substitution/inverse-substitution transform unit successively performing an inverse substitution of the upper 64-bit data, and outputting the inverse-substituted upper 64-bit data to a first demultiplexer, an add-round-key transform unit successively performing an addition of the upper 64-bit data outputted through a decryption output terminal of the first demultiplexer to an upper 64-bit round key generated by the round key generation unit, and outputting the added upper 64-bit data to a third demultiplexer, and a mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added upper 64-bit data, outputting the inverse-mixcolumn-transformed upper 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed upper 64-bit data in a 64-bit data register; and

when a second clock of the round operation start signal becomes '1' , the shift/ inverse-shift_row transform unit performing a byte-inverse-shift of lower 64-bit data of the 128-bit input data inputted through the bus and outputting the byte-inverse-shifted lower 64-bit data through the first multiplexer, the substitution/ inverse-substitution transform unit successively performing an inverse substitution of the lower 64-bit data, and outputting the inverse-substituted lower 64-bit data to the first demultiplexer, the add-round-key transform unit successively performing an addition of the lower 64-bit data outputted through the decryption output terminal of the first demultiplexer to a lower 64-bit round key generated by the round key generation unit, and outputting the added lower 64-bit data to the third demultiplexer, the mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added lower 64-bit data, outputting the inverse-mixcolumn-transformed lower 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed lower 64-bit data in lower 64 bits of a 128-bit data register, and simultaneously storing the upper 64-bit data stored in the 64-bit data register in upper 64 bits of the 128-bit data register.

[27] The decryption method as claimed in claim 26, wherein at the step of the round key generation unit transforming the 128-bit input key into the 128-bit round key for decryption in accordance with the value of the mode signal inputted through the bus, and storing the 128-bit round key in the internal 128-bit round key register, the 128-bit round key for decryption is generated in a period of one clock of the round operation start signal